AZ

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-259716
(43)Date of publication of application : 13.09.2002

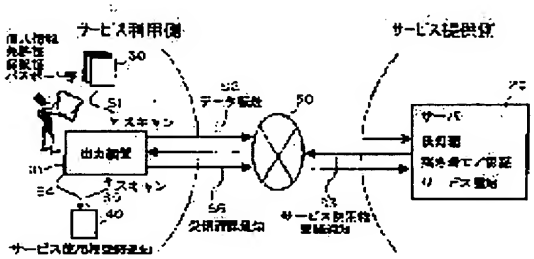
(51)Int.Cl. G06F 17/60
G06F 12/14

(21)Application number : 2001-053372
(22)Date of filing : 28.02.2001

(71)Applicant : RICOH CO LTD
(72)Inventor : MURATA MIKUNI
KEGI SHUNZO
TANIGAWA TETSUO

(54) SERVICE USER IDENTIFYING METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To establish a service user identifying method for an information providing service using a network in which a service provider issues a service use right acceptance notification to allow any service user to use only a certain service (no password entry) to serve for identification of the service user.
SOLUTION: An output device 10 having a reading function and a server 20 are connected through the network 50, and the output device 10 reads the ID card 30 such as driver license, insurance certificate, passport, etc., (S1), and sends the read ID card 30 to the server 20 through the network 50. The server 20 makes checkup and verification between the individual information contained in the ID card 30 and the previously registered individual information of the service user, and if the data are identical, the service use right acceptance notification is sent to the output device 10 and the service user is identified.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－259716
(P2002－259716A)
(43)公開日　平成14年９月13日(2002.9.13)

(51)Int.Cl.'	識別記号	FI	テーマコード'(参考)
G06F 17/60	302	G06F 17/60	302E 5B017
	326		326
	330		330
	512		512
12/14	320	12/14	320C

審査請求　未請求　請求項の数5　ＯＬ　（全８頁）

(21)出願番号　特願2001－53372(P2001－53372)

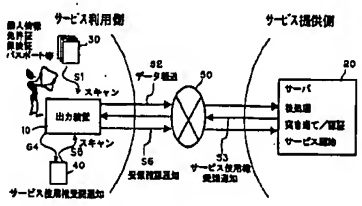
(22)出願日　平成13年２月28日(2001.2.28)

(71)出願人　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号
(72)発明者　村田　巳晋
東京都大田区中馬込１丁目３番６号　株式会社リコー内
(72)発明者　毛木　俊三
東京都大田区中馬込１丁目３番６号　株式会社リコー内
(74)代理人　100079843
弁理士　高野　明近　（外２名）

最終頁に続く

(54)【発明の名称】　サービス利用者特定方法

(57)【要約】
【課題】　ネットワークを利用した情報提供サービスにおいて、サービス提供者がサービス利用者に当該サービスのみ使用可能なサービス使用権受諾通知を発行し（パスワード入力なし）、サービス利用者を特定する。
【解決手段】　読み取り機能を有する出力装置１０とサーバ２０は、ネットワーク５０を介して接続され、出力装置１０は、免許証、保険証、パスポート等の身分証明書３０をを読み取って（Ｓ１）、読み取った身分証明書３０をネットワーク５０を介してサーバ２０に送信する。サーバ２０は、送信された身分証明書３０の個人情報と予め登録しているサービス利用者の個人情報とを突き当て／認証を行って、データが合致した場合に、出力装置１０にサービス使用権受諾通知４０を送信し、サービス利用者を特定する。



【特許請求の範囲】
【請求項１】　ＭＦＰ、プリンタ等の出力装置とサービスを提供するサービス提供側装置とがネットワークを介して接続され、前記出力装置を用いてサービス提供者がサービス利用者を特定するサービス利用者特定方法であって、前記出力装置は、読み取り機能を有し、サービス利用者がサービス提供者の提供するサービスを利用する際に、サービス利用者自身の免許証、保険証、パスポート等の公的な身分証明書を読み取り、読み取った身分証明書の記載内容をネットワークを介して前記サービス提供側装置に送信し、送信された身分証明書の記載内容に基づいてサービス提供者がサービス利用者を特定することを特徴とするサービス利用者特定方法。
【請求項２】　請求項１において、前記出力装置または前記サービス提供側装置は、複数の情報を自動認識する機能を有し、前記身分証明書に記載されている複数のＩＤ情報を自動認識し、自動認識された複数のＩＤ情報と前記サービス提供側装置に登録されているサービス利用者のＩＤ情報とを該サービス提供側装置により突き合わせて、サービス提供者がサービス利用者を特定する確度を向上させることを特徴とするサービス利用者特定方法。
【請求項３】　請求項１において、前記身分証明書の記載内容に基づいてサービス提供者によりサービス利用者が特定されると、当該サービスのみサービス受諾を承認するためのパスワードが前記サービス提供側装置により生成され、前記出力装置は、紙出力機能を有し、該生成されたパスワードを前記サービス提供側装置からネットワークを介して受信し、受信したパスワードを紙に出力し、サービス利用者が当該サービスを利用する際に、前記出力した紙に記録されたパスワードを読み取り、読み取ったパスワードをネットワークを介して前記サービス提供側装置に送信し、送信されたパスワードに基づいてサービス提供者がサービス利用者を特定することを特徴とするサービス利用者特定方法。
【請求項４】　請求項３において、前記サービス提供側装置は、前記パスワードを、前記出力装置の読み取り機能により読み取り可能な状態で暗号化することを特徴とするサービス利用者特定方法。
【請求項５】　ＭＦＰ、プリンタ等の出力装置とサービスを提供するサービス提供側装置とがネットワークを介して接続され、前記出力装置を用いてサービス提供者がサービス利用者を特定するサービス利用者特定方法であって、前記出力装置は、携帯端末装置に関する固有情報を受信可能なＦＡＸ受信機能を有し、サービス利用者が携帯端末装置を用いて当該サービスを利用する際に、サービス利用者の携帯端末装置に関する固有情報を公衆回線を介して受信し、受信した携帯端末装置に関する固有情報をネットワークを介して前記サービス提供側装置に送信し、送信された携帯端末装置に関する固有情報に基づいてサービス提供者がサービス利用者を特定することを特徴とするサービス利用者特定方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、サービス利用者特定方法、より詳細には、ネットワークを利用した情報提供サービスにおけるサービス利用者特定方法に関し、読み取り機能を有するＭＦＰ、プリンタ等の出力装置を利用したシステムに関する。
【０００２】
【従来の技術】従来技術に関して、例えば、特開平１１－３３８６５８号公報（データ管理システム）には、蓄積管理する処理データをユーザビリティの高いデータ処理装置に出力できるようにして、処理データを蓄積管理するシステムの利用性を向上させるシステムが記載されているが、機器固有情報のみを管理するために、サービス利用者の特定が困難という問題点がある。
【０００３】また、特開２０００－２０４７１号公報（情報機器ネットワークシステム、その照合方法、情報機器および記憶媒体）には、各機器からユーザ情報の確認をサーバに行わせることで、ユーザ情報管理の時間的損失を減らせる情報機器ネットワークシステムが記載されており、オペレータ（利用者）がパスワードを入力すると、第三者から覗かれ、盗用される危険の回避が困難という問題点がある。
【０００４】
【発明が解決しようとする課題】現在、ＩＴ環境の発達により、ＰＣやＭＦＰ，プリンタが常設されたオフィスや自宅だけでなく、例えば、ビジネスコンビニエンスストアやコンビニエンスショップといった公共の場所に移動中に立ち寄るモバイルワーカーが、店内に設置されているＭＦＰ、プリンタ等の出力装置を用いてハードコピーの形態で情報やチケット等の有価証券を入手可能なサービスが行われようとしている。
【０００５】上記サービスを実施する際、サービス提供者は、情報や有価証券の対価として課金を行うことや、後の請求・回収にまつわるトラブルの発生防止やトラブル発生時の紛争解決を目的に課金内容の証明を行う必要があるため、支払い者となる利用者や契約者を特定する必要がある。
【０００６】その手段として、利用者がサービスを申し込む時に、事前にサービス提供者と利用者が共有化したパスワードを入力することが一般的である。しかし、公共の場所において、例えば、有価証券の偽造といった悪用を避けるため、周囲を遮蔽することができないこともあり、そこに設置されるカラー出力機器に１０キー等で入力するときに、第三者から覗かれ、盗用される危険が回避できない。
【０００７】代替手段として、例えば、磁気を用いた不可視情報により利用者情報を記録したＩＤカードを、サ

ービス提供者から利用者に対して事前に提供し、利用時に読み取り装置で利用者情報を読み取り、サービス提供者に送る手段があるが、ＩＤカードが盗難されたり紛失した場合、１０キー等でパスワードを入力する行為との組み合わせにより悪用されるリスクを低減しなければ、盗用される危険が著しく拡大することになる。

【０００８】本発明は、上述の点に鑑みてなされたものであり、ネットワークを利用した情報提供サービスにおけるサービス利用者の安全性を向上させること、を目的としてなされたものである。

【０００９】

【課題を解決するための手段】請求項１の発明は、ＭＦＰ、プリンタ等の出力装置とサービスを提供するサービス提供側装置とがネットワークを介して接続され、前記出力装置を用いてサービス提供者がサービス利用者を特定するサービス利用者特定方法であって、前記出力装置は、読み取り機能を有し、サービス利用者がサービス提供者の提供するサービスを利用する際に、サービス利用者自身の免許証、保険証、パスポート等の公的な身分証明書を読み取り、読み取った身分証明書の記載内容をネットワークを介して前記サービス提供側装置に送信し、送信された身分証明書の記載内容に基づいてサービス提供者がサービス利用者を特定することを特徴としたものである。

【００１０】請求項２の発明は、請求項１において、前記出力装置または前記サービス提供側装置は、複数の情報を自動認識する機能を有し、前記身分証明書に記載されている複数のＩＤ情報を自動認識し、自動認識された複数のＩＤ情報と前記サービス提供側装置に登録されているサービス利用者のＩＤ情報とを該サービス提供側装置により突き合わせて、サービス提供者がサービス利用者を特定する確度を向上させることを特徴としたものである。

【００１１】請求項３の発明は、請求項１において、前記身分証明書の記載内容に基づいてサービス提供者によりサービス利用者が特定されると、当該サービスのみサービス受諾を承認するためのパスワードが前記サービス提供側装置により生成され、前記出力装置は、紙出力機能を有し、該生成されたパスワードを前記サービス提供側装置からネットワークを介して受信し、受信したパスワードを紙に出力し、サービス利用者が当該サービスを利用する際に、前記出力した紙に記録されたパスワードを読み取り、読み取ったパスワードをネットワークを介して前記サービス提供側装置に送信し、送信されたパスワードに基づいてサービス提供者がサービス利用者を特定することを特徴としたものである。

【００１２】請求項４の発明は、請求項３において、前記サービス提供側装置は、前記パスワードを、前記出力装置の読み取り機能により読み取り可能な状態で暗号化することを特徴としたものである。

【００１３】請求項５の発明は、ＭＦＰ、プリンタ等の出力装置とサービスを提供するサービス提供側装置とがネットワークを介して接続され、前記出力装置を用いてサービス提供者がサービス利用者を特定するサービス利用者特定方法であって、前記出力装置は、携帯端末装置に関する固有情報を受信可能なＦＡＸ受信機能を有し、サービス利用者が携帯端末装置を用いて当該サービスを利用する際に、サービス利用者の携帯端末装置に関する固有情報を公衆回線を介して受信し、受信した携帯端末装置に関する固有情報をネットワークを介して前記サービス提供側装置に送信し、送信された携帯端末装置に関する固有情報に基づいてサービス提供者がサービス利用者を特定することを特徴としたものである。

【００１４】

【発明の実施の形態】図１は、本発明が適用されるサービス利用者特定フローの一例を説明する図で、図中、１０は、サービス利用側装置である読み取り機能を有するＭＦＰ、プリンタ等の出力装置、２０は、サービス提供側装置であるサーバ、３０は、個人情報が記載された免許証、保険証、パスポート等の身分証明書、４０は、サービス使用権受諾通知、５０は、ネットワークである。まず、出力装置１０で身分証明書３０をスキャンし（Ｓ１）、前処理として、一次加工（データ補正：ＭＴＦ等）を行った後、出力装置１０の入力データ処理／解析部にて、例えば、像域分離、パターン認識、色相差認識、文字認識、暗号認識といった二次加工を行うことも出来るが、一次加工したデータをネットワーク５０を介してサーバ２０に送信し（Ｓ２）、後処理として、上記二次加工をサーバ２０にて行うことも出来る。また、二次加工は、データを認識後、個人認証に必要な情報のみを選別し、情報の属性に添付するまでを行うが、出力装置１０とサーバ２０で分担して行うこともできる。

【００１５】このことは、例えば、ＩＳといった規格により認証フォーマットが成立し、そのフォーマットに装置が対応することで汎用的に認証可能となる場合、または、認証フォーマットは未成立だが、装置やサービスを提供する企業間での個別対応により認証を行う場合のいずれにも対応可能とするためである。

【００１６】また、こういったフォーマットは暫時変化していくことが想定されるが、サービス利用側機器とサービス提供側機器のいずれかもしくは両方の、ソフトウェアやシステム（ハードウェアを含む）を変更することにより、柔軟に対応可能とすることができる。

【００１７】また、ネットワークを介したデータのやりとりを行う際、ネットワークの能力によって処理速度が大きく左右される。当然、サービス利用者、サービス提供者の双方にとって、可能な限り短時間での処理が必然的なニーズとなる。その際、上述のような自由度の高いシステム構成を活用することにより処理時間を最短化することが可能である

【００１８】本例では、出力装置１０から送信されたデータの二次加工をサーバ２０にて行った後に、サーバ２０が保持しているサービス利用者の個人情報と突き当て／認証を行って、データが合致した場合に、出力装置１０にサービス使用権受諾通知４０を送信する（Ｓ３）。出力装置１０は、受信したサービス使用権受諾通知４０を紙に出力し（Ｓ４）、サービス利用者がサービス使用権受諾通知４０に同意の意思表明として、例えば、サイン、捺印をした後に、サービス使用権受諾通知４０を出力装置１０でスキャンして（Ｓ５）、受領確認通知としてサーバ２０へネットワーク５０を介して送信し（Ｓ６）、サービス提供者は、サービス利用者に対してサービスを開始する。

【００１９】（実施例）図２は、本発明が適用されるシステム構成例を示すブロック図で、出力装置１０は、ユーザＩ／Ｆ部１１、紙出力部１２、紙入力部１３、通信Ｉ／Ｆ部１４、機器固有情報記憶部１５、サービス関連情報記憶部１６、入力データ処理／解析部１７を有し、サーバ２０は、データ参照部２１、入力データ処理／解析部２２を有する。

【００２０】図３は、本発明が適用されるサービス利用者特定フローの一例を説明するフローチャートである。まず、サービス利用者がサービスを利用するときに、公的に自己を証明可能な免許証、保険証、パスポート等の身分証明書の表紙や該当ページを開き、公共の場所に設置されている出力装置１０のスキャナ上に載せ、例えば、スタートキーを押下げるといった開始の指示をするだけで、人手を介さず行われる。

【００２１】スキャナ機能を有する出力装置１０は、載せられた書類のサイズや内容を、センス手段で認識し、どのような証明書か種類を特定することができる。通常、種類特定後、スキャンを行うが、種類特定を目的として行うセンスと同時にスキャンしたり、スキャンを先行し、後に種類特定を行うことも可能である。

【００２２】一次加工条件を含むスキャン条件は、あらかじめ最適化されているが、載せられた書類の特性に合わせて自動的もしくは手動にて最適化することも可能である。

【００２３】次に、出力装置１０の入力データ処理／解析部１７にて一次加工後（ステップＳ１２）、符号化を行って（ステップＳ１３）、機器固有情報記憶部１５から機器固有情報を取得し、サービス関連情報記憶部１６からデータの送信先を取得して、これらを認識する（ステップＳ１４）。出力装置１０は、処理解析済みまたは未処理のデータと、ステップＳ１４で認識した機器固有情報とをネットワーク５０を介してサーバ２０に送信する（ステップＳ１５）。データを受信したサーバ２０は、入力データ処理／解析部２２にて二次加工を施して（ステップＳ１６）、データの処理／解析を行う。

【００２４】ここで、身分証明書３０の特徴は、書式が固定化されているので、どのような証明書か種類を特定

すれば、どの部位に何が記載されているか判断できる点にある。各証明書に必ず存在する特徴的なイメージを検出し、そこからの位置情報で、利用者特定に必要な情報を任意の数認識し、変換することができる。

【００２５】また、前述したように、二次加工は、出力装置１０、サーバ２０の双方で行うことができる。出力装置１０から通信ネットワーク５０を介してサーバ２０にデータ転送後、サーバ２０内のデータ参照部２１にて、予め登録されているサービス利用者の個人情報を参照し、確認して（ステップＳ１７）、出力装置１０から転送された個人データと、サーバ２０内に登録されているサービス利用者の個人情報とが合致するかどうか突き合せを行って（ステップＳ１８）、合致した場合（ＹＥＳの場合）は、サーバ２０からサービス使用権受諾通知４０が、ネットワーク５０を介して出力装置１０に対して送信される（ステップＳ１９）。

【００２６】一方、出力装置１０から転送された個人データと、サーバ２０内に登録されているサービス利用者の個人情報が合致しなかった場合（ＮＯの場合）は、サーバ２０から、例えば、警備区、警察、サービス提供者監視区といった所定の関係各所に警告情報が送信される（ステップＳ２０）。尚、この一連の処理は、サービス利用者が有する身分証明書３０の表紙や該当ページを開き、公共の場所に設置されている出力装置１０のスキャナ上に載せ、例えば、スタートキーを押下げるといった開始の指示をするだけで、人手を介さず行われる。

【００２７】また、他の実施例として、前述したステップＳ１８でサーバ２０内のデータ参照部２１にて、二次加工後のサービス利用者の個人データと予め登録されているサービス利用者の個人情報と突き合せを行う際、限られた少数の情報ではなく、複数の情報と突き合せを行って、特定の確度を上げるために、図３に示すサブフローのように、予め登録されているサービス利用者の複数のデータを検出し（ステップＳ２１）、サーバ２０内のデータ参照部２１にて、順次もしくは同時に突き合せを行う（ステップＳ２２）。

【００２８】ここで、二次加工等の事前の処理において、一つの身分証明書３０の表紙や該当ページから、複数の特定に必要な情報を認識可能であることが重要となる。また、場合によっては、複数の身分証明書３０を連続もしくは同時にスキャンし、それらをまたがった突き合せを行うことにより、更に特定の確度を向上させることが可能である。

【００２９】図４は、本発明が適用されるシステム構成例を示すブロック図である。図５は、本発明が適用されるサービス利用側のサービス依頼フローの一例を説明するフローチャートである。サービス利用者とサービス提供者間において、後に発生する可能性が有る請求回収時のトラブルを防止するために、サービス利用者がサービス提供に関して同意した証拠を残すことが必要となる場

7

合がある。それに加え、利用者特定の確度の更なる向上が必要な場合に有効な方法を以下に示す。

【００３０】まず、利用者特定の次段階として、出力装置１０が有する紙出力機能を用いてサーバ２０から伝送されたサービス使用権受諾通知４０を出力する（ステップＳ３１）。サービス利用者は、出力されたサービス使用権受諾通知４０に、同意の意思表示としてサイン、捺印等を施すが（ステップＳ３２）、ここで、当然確認のみの場合もある。次に、サービス使用権受諾通知４０を出力装置１０のスキャナ上に載せ開始の指示をする（ステップＳ３３）。ここで、サービス提供者は、サービス使用権受諾通知４０にそのサービス利用時のみ有効なパスワードとして、例えば、数字やバーコードを付加しておくことにより更に特定の確度向上を行うことができる。次に、出力装置１０の入力データ処理／解析部１７にて一次加工後（ステップＳ３４）、処理解析済みまたは未処理のデータと、出力装置１０の固有情報とをネットワーク５０を介してサーバ２０に送信する（ステップＳ３５）。データを受信したサーバ２０は、入力データ処理／解析部２２にて二次加工を施して（ステップＳ３６）、データの処理／解析を行う。

【００３１】サーバ２０内のデータ参照部２１にて、予め登録されているサービス利用者へ提供したパスワード、暗号情報を参照し、確認して（ステップＳ３７）、出力装置１０から転送されたサービス使用権受諾通知４０に付加されたパスワードと、サーバ２０内に登録されているサービス利用者のパスワードとが合致するかどうか突き合せを行って（ステップＳ３８）、合致した場合（ＹＥＳの場合）は、サービス提供者が提供するサービスがサーバ２０よりネットワーク５０を介して出力装置１０に対して送信される（ステップＳ４０）。

【００３２】一方、サービス使用権受諾通知４０に付加されたパスワードとサーバ２０内に登録されているサービス利用者のパスワードとが合致しなかった場合（ＮＯの場合）は、サーバ２０から、例えば、警備区、警察、サービス提供者監視区といった所定の関係各所に警告情報が送信される（ステップＳ３９）。

【００３３】また、サービス提供者は、サービス利用者がサービス使用権受諾通知４０に施した同意の意思表明としてのサインや捺印を利用者特定の情報として活用することもできる。

【００３４】上記パスワードとして数字やバーコード以外に、サービス使用権受諾通知４０に人が容易に判読できない、もしくは、見ることができない暗号で記録し、さらに、サービス使用権受諾通知４０にサービスメニューを付加し、そのサービスメニューからサービス選択を行なった後、サービス使用権受諾通知４０をスキャンし、サービス依頼を行なう手順や、出力装置１０から直接サーバ２０にサービス使用権受諾通知４０の発行依頼を行ったり、出力装置１０が直接サービス使用権受諾通知４０の発行を行うといった手順も考えられ利用手順を最短化することも可能である。

8

【００３５】図６は、本発明が適用されるシステム構成例を示すブロック図で、図中、６０は、携帯電話、７０は、公衆回線である。サービス利用者が所有する携帯電話６０の固有情報は、予めサーバ２０に登録されており、図６に示すように、サービス利用者は、携帯電話６０を用いて公衆回線７０を介して出力装置１０のＦＡＸ番号に電話をかける。サーバ２０は、サービス利用者の携帯電話６０から提供された機器固有情報を認識し、その情報をサーバ２０へ転送する。

【００３６】図７は、本発明が適用されるサービス利用側のサービス依頼フローの一例を説明するフローチャートである。まず、サービス利用者は、サーバ２０に登録されているサービス利用者が所有する携帯電話６０を利用して公衆回線７０を介して出力装置１０のＦＡＸ番号に電話をかけ（ステップＳ５１）、出力装置１０は、携帯電話６０の例えば、電話番号、所有者の住所、氏名といった固有情報を認識し（ステップＳ５３）、認識した携帯電話６０の固有情報と出力装置１０の固有情報とをネットワーク５０を介してサーバ２０に送信する（ステップＳ５４）。サーバ２０は、サーバ２０内のデータ参照部２１にて、予め登録したサービス利用者の携帯電話６０の固有情報を参照し、確認して（ステップＳ５５）、出力装置１０から転送された携帯電話６０の固有情報とサーバ２０内に登録されているサービス利用者の個人情報と合致するかどうか突き合せを行って（ステップＳ５６）、合致した場合（ＹＥＳの場合）は、サーバ２０からサービス使用権受諾通知４０が、ネットワーク５０を介して出力装置１０に対して送信される（ステップＳ５８）。

【００３７】一方、ステップＳ５６で合致しなかった場合（ＮＯの場合）は、サーバ２０から、例えば、警備区、警察、サービス提供者監視区といった所定の関係各所に警告情報が送信される（ステップＳ５７）。

【００３８】

【発明の効果】請求項１の発明によると、サービス利用者は、パスワードを公共の場所において１０キー等で入力する必要が無く、第三者から覗かれ、盗用される危険を回避できる。

【００３９】請求項２の発明によると、サービス提供者は、複数の情報による利用者特定が可能となり、サービス利用者の免許証，保険証等の身分証明書の偽造による悪用を防止できる。

【００４０】請求項３の発明によると、サービス利用者は、パスワードを公共の場所において１０キー等で入力する必要が無く、第三者から覗かれ、盗用される危険を回避でき、サービス提供者から提供されるパスワードは、サービス利用時毎に改訂可能なため、盗用へのリスクが軽減でき、サービス提供者にとっても、そのパスワードをサービス利用者のサービス利用受諾証明としても使用することができる。

9

【００４１】請求項４の発明によると、サービス利用者は、第三者から覗かれても、判読不可能な状態に暗号化されたパスワードにより、盗用を防止することができる。

【００４２】請求項５の発明によると、サービス利用者は、パスワードを公共の場所において１０キー等で入力する必要が無く、第三者から覗かれ、盗用される危険を回避できる。

【図面の簡単な説明】

【図１】　本発明が適用されるサービス利用者特定フローの一例を説明する図である。

【図２】　本発明が適用されるシステム構成例を示すブロック図である。

【図３】　本発明が適用されるサービス利用者特定フローの一例を説明するフローチャートである。

10

＊【図４】　本発明が適用されるシステム構成例を示すブロック図である。

【図５】　本発明が適用されるサービス利用側のサービス依頼フローの一例を説明するフローチャートである。

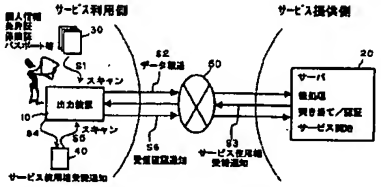
【図６】　本発明が適用されるシステム構成例を示すブロック図である。

【図７】　本発明が適用されるサービス利用側のサービス依頼フローの一例を説明するフローチャートである。

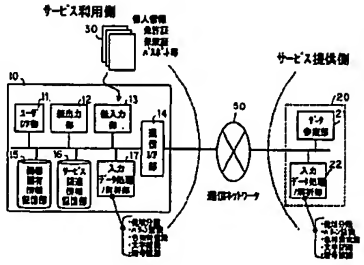
【符号の説明】

１０…出力装置、１１…ユーザＩ／Ｆ部、１２…紙出力部、１３…紙入力部、１４…通信Ｉ／Ｆ部、１５…機器固有情報記憶部、１６…サービス関連情報記憶部、１７…入力データ処理／解析部、２０…サーバ、２１…データ参照部、２２…入力データ処理／解析部、３０…身分証明書、４０…サービス使用権受諾通知、５０…通信ネットワーク、６０…携帯電話、７０…公衆回線。

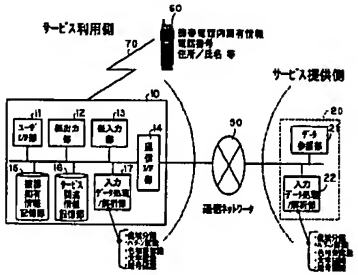
【図１】



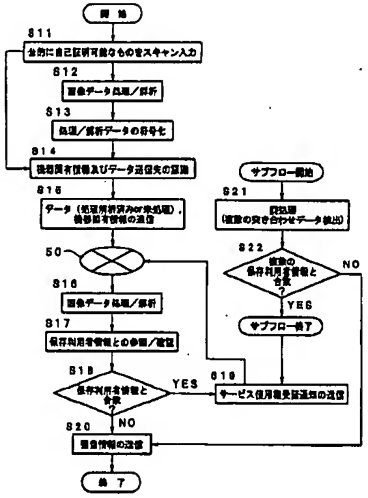
【図２】



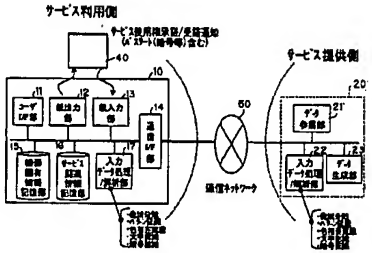
【図６】



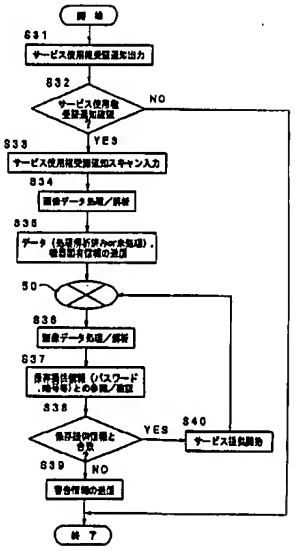
【図３】



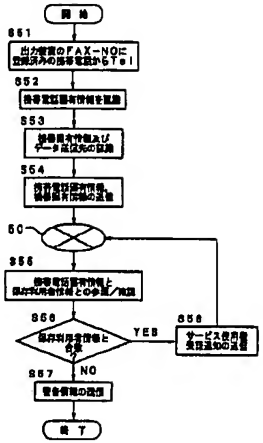
【図４】



【図５】



【図７】



フロントページの続き

(72)発明者 谷川 哲郎
東京都大田区中馬込１丁目３番６号 株式
会社リコー内

Fターム(参考) 5B017 AA03 BA05 BA09 CA15 CA16